ANALYSIS

29(107), March 1, 2015

ISSN 2278–5469 EISSN 2278–5450

Discovery

Image encryption and decryption using advanced encryption algorithm

Ramaraju PV, Nagaraju G, Chaitanya RK

1.Professor, Department of ECE, SRKR Engineering College, Bhimavaram, India; Email: pvrraju50@gmail.com
2.Asst.Professor, Department of ECE, SRKR Engineering College, Bhimavaram, India; Email: bhanu.raj.nikhil@gmail.com
3.Asst.Professor, Department of ECE, SRKR Engineering College, Bhimavaram, India; Email: rkc639@gmail.com

Publication History
Received: 07 January 2015
Accepted: 12 February 2015
Published: 1 March 2015

Citation
Ramaraju PV, Nagaraju G, Chaitanya RK. Image Encryption and Decryption using Advanced Encryption Algorithm. *Discovery*, 2015, 29(107), 22-28

ABSTRACT

Today with the rapid use of computer technology information processing became very easy in the same way the problem of information security is increasing. This paper deals with the secrecy of images, so image encryption is the best technique for information hiding. The novelty of the work lies in generating key images for encryption. Here the key image is created with the help of secret alphanumeric keyword. Each alphanumeric key will be having a unique 8bit value generated by Binary key table. Problem is to be investigated and resolved is how to get the image encryption algorithm which is simple yet safe, with the lightweight and efficient computing. This encryption algorithm which combines Playfair cipher and the Vigenere cipher gives better results. The experimental results showed a correlation between the elements of the image after encryption has decreased significantly. The average of quality of encryption showed that the rate of change of image pixels is high enough so that cipher image difficult to identify. The resulting image is found to be more distorted in this technique. By applying the reverse process we get the decrypted image.

Keywords: carrier image, encryption, decryption, binary key table, super encryption.

1. INTRODUCTION

Digital image processing techniques help in manipulation of the digital images by using computers. As raw data from imaging sensors from satellite platform contains deficiencies. To get over such flaws and to get originality of information, it has to undergo various phases of processing. The three general phases that all types of data have to undergo while using digital technique are Pre- processing, enhancement and display, information extraction. Day by day the progress of information age, causes for the leakage of certain valuable information, so a new technique should be developed for preventing the information leakage. For digital data technique had been developed that is encrypting it which is converting data of readable form into non readable form, so that if a hacker hack the information he cannot understand it until he know the decryption technique and decryption password[1].

Cryptography

More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, authentication and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Here Fig 1 shows the model of encryption and decryption processes for data.

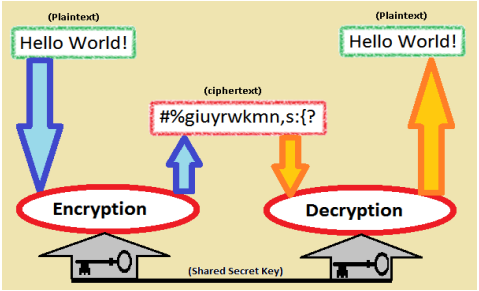


Figure 1 Model of encryption and decryption

Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. According to this they will choose a cipher which means a secret key with the help of that cipher they will encrypt the message. In a Caesar cipher, each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, A would become D, B would become E, Y would become B and so on. The Vigenere cipher consists of several Caesar ciphers in sequence with different shift values. Playfair Cipher scheme was invented by Charles Wheatstone in 1854. However, eventually the scheme came to be known by the name of Lord Playfair. The Playfair Cipher, also called as Playfair Square, is a cryptographic technique that is used for manual encryption of data. These schemes are therefore termed computationally secure theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. G.Prasanna Lakshmi, Dr. D.A.Chandulal, Dr.KTV Reddy proposed Visual Cryptography which is a type of cryptography which encodes a number of images in the way that when the images on transparencies are stacked together, the hidden message appears without a trace of original images[2]. K.Sakthidasan and B.V.Santhosh Krishna have presented the method of image encryption scheme which employs one of the three dynamic chaotic systems (Lorenz or Chen or LU chaotic system selected based on 16-byte key) to shuffle the position of the image pixels, thereby significantly increasing the resistance to attacks[3]. Chao-Shen Chen and Rong-jain Chen proposed an image encryption and decryption algorithm based on SCAN methodology[4]. Xinpeng Zhang, Guorui Feng, Yanli Ren, and Zhenxing Qian proposed a novel scheme of scalable coding for encrypted images[5]. Panduranga H.T, Naveenkumar S.K proposed A novel 3-step combinational approach for image encryption[6]. Sinha, K. Sing proposed A technique for image encryption using digital signature[7]. Panduranga H.T, Naveenkumar S.K proposed A novel image encryption method using 4outof8 code[8]. G. Nagaraju, T. V. Hymalakshmi have presented the method of Image Encryption using Secret-Key images and SCAN Patterns[9].

Need for security

Encrypting data on mobile devices eliminates the dangers associated with loss or theft. The process makes data worthless to unauthorized users. Typically, by processing data through a mathematical formula called an algorithm, encryption software converts data into "cipher text". Following this conversion, that data requires users to input their unique credentials to gain access to it. Provided those credentials stay private, they make it virtually impossible for others to access the data. Most initial computer applications had no or at best, very little security. This continued for a number of years until the importance of data was truly realized. Until then, computer data was considered to be useful, but not something to be protected. When computer applications were developed to handle financial and personal data, the real need for security was felt like never before. People realized that data on computers was an extremely important aspect of modern life. Therefore, various areas in security began to gain prominence.

Two typical examples of such security mechanisms were as follows:

Provide a user id and password to every user and use that information to authenticate a user. Encode information stored in the databases in some fashion so that it is not visible to users who do not have the right permission. As technology improved, the communication infrastructure became extremely mature and, newer and newer applications began to be developed for various users demands and needs. Soon, people realized that the basic security measures were not quite enough. Furthermore, the Internet took the world by storm and there were many examples of what could happen if there was insufficient security built in applications developed for the internet. So the methods have developed to protect the information passing through the internet.

So here we are proposing a new algorithm called advanced encryption algorithm where we are going to use two carriers. Carrier1 or playfair cipher and carrier2 or vigenere cipher, carrier2 is generated with the help of carrier1 and using key stream generators. The technique of using two carriers is to provide double security so better quality of encryption. This algorithm mainly includes two phases

- Generation of carrier1 and carrier2 ciphers
- Applying them to images

Generation of carrier ciphers

With the user entered password a carrier1 cipher is generated, initially we will assign values for all alphabets, small a-z and capital A-Z and numbers from 0-9 and some special symbols, in the range of 0 to 255, so when the user enter the password with the help of it a 200 by 200 size carrier1 image is generated. Carrier2 cipher is developed using the carrier1 image and with the help of key stream generator which is in the form of Ki=(K(i-1)+K(i-m))mod256. The value of m depends up on the person who written the code it should not be more than intensity value present at(1,1) position of carrier1 image, because in carrier2 we will keep same intensity values of carrier1 up to intensity value present in (1,1) position of carrier1 image and there after key stream generator is implemented.

Applying them to image

Convert image intensity values to binary and also carrier1 cipher and carrier2 cipher values to binary. Now perform XOR operation of original image and carrier1 cipher, the resultant obtained is XORed with carrier2 cipher. Now the result is again converted to decimal and reshaped to a 200by200 matrix and transmitted. In decryption we have to perform reverse logic remember that for performing Xor we have to convert decimal into binary values.

2. CARRIER IMAGE GENERATION

For any encryption process, in the process of encryption we have to generate carry image but here we are going to generate two carry images carry image1 which is also called play fair cipher carry image2 which is also called vigenere cipher. Carry image 2 is generated with the help of carry image1 so, No need to worry hence we have to concentrate on carry image 1 generation. The carry image1 is generated with the help of password given by user it may consist of capital letters or small letters or numbers and some special characters which are listed in the table1. Now we will assign numbers ranging from 0 to 255 for the above input characters. We generate keys by using the alphabet codes that is either alphabets or numbers. We can generate different types of carrier images using the different keys generated by this alphabet codes. As we enter the different keywords, each keyword is taken and rearranged in a matrix form of size equal to the size of original image. If the length of the keyword is very small then the same keyword is repeated till the length is become equal to size of original image. By using luck up table of the alphabet character as shown in table1, a carrier image is created. Depending upon the keyword, carrier image1 is generated and used in the encryption process to generate a encrypted image. Here in generation of encryption process we have to see that different values between0 to 255 should be assigned to different input characters if same value is assigned to different variables our quality of encryption will be decreases. The values we are assigning should cover the entire 0 to 255 range for better quality of encryption and also password we are entering should not be less than 8 characters. The code will accept the password if it is less than 8 characters but fo better security reasons we will maintain a minimum 8 bit password.

Binary key table

Table 1 Assigning of binary numbers to alphabets, numbers and symbols

S.NO	ALPHANUMERALS	DECIMAL	BINARY
1	a	7	00000111
2	A	11	00001101
3	b	19	00010011
4	B	27	00011011
5	c	35	00100011
6	C	43	00101011
7	d	55	00110111
8	D	63	00111110
9	e	77	01001101
10	E	93	01011101
11	f	101	01100110
12	F	109	01101101
13	g	117	01110101
14	G	129	10000001

15	H	137	10001001
16	H	143	10001111
17	i	151	10010111
18	I	163	10100011
19	j	171	10101011
20	J	183	10110111
21	k	191	10111111
22	K	201	11001001
23	l	211	11010011
24	L	223	11011111
25	m	243	11110011
26	M	255	11111111
27	n	8	00001000
28	N	12	00001010
29	o	28	00011010
30	O	32	00100000
31	p	42	00101010
32	P	54	00110110
33	q	62	00111110
34	Q	76	01000100
35	r	82	01001010
36	R	94	01011110
37	s	102	01100110
38	S	116	01110100
39	t	128	10000000
40	T	136	10001000
41	u	142	10001110
42	U	156	10011100
43	v	162	10100010
44	V	176	10110000
45	w	182	10110110
46	W	192	11000000
47	x	206	11001110
48	X	218	11011010
49	y	226	11100010
S.NO	**ALPHABETS**	**DECIMAL**	**BINARY**
50	Y	236	11101010
51	z	242	11110001
52	Z	254	11111110
53	0	20	00010100
54	1	40	00101000
55	2	60	0011110
56	3	80	01010000
57	4	100	01100100
58	5	120	01111000
59	6	160	10100000
60	7	180	10100100
61	8	200	11001000
62	9	220	11011100
63	!	241	11110001
64	@	244	11110100
65	#	245	11110101
66	$	246	11110110
67	%	247	11110111
68	^	248	11111000
69	&	250	11111010
70	*	251	11111011
71	.	252	11111100

Generation of carrier 2 is simple, suppose if the carrier 1 (1,1) position is 87(just assume only) up to 87 values carrier2 is same as carrier1and from 88 to 40000 values they are changed using help of key stream generator Ki=K(i-1)+K(i-m)mod256. The value of m is depend up on yourself, remember value of 'm' should not be greater than or equal to value of intensity at(1,1) thus carrier2 also generated. Let us see the images for carrier 1 and carrier2 for different passwords. Examples for Carrier images for two different passwords are given fig. 2

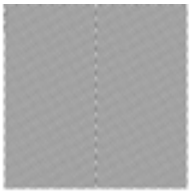
ENCRYPTION PASSWORD: **elegants@2014**

Carrier 1 playfair cipher

Carrier 2 vigenere cipher

ENCRYPTION PASSWORD: **andhrauniversity**

Carrier 1 playfair cipher



Carrier 2 vigenere cipher

Figure 2 Carrier images for two different passwords

3. PROPOSED ADVANCED ENCRYPTION SYSTEM ENCRYPTION

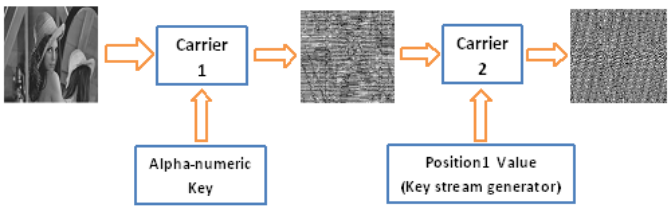


Figure 2 Process of encryption

Encryption algorithm

The proposed encryption process can be seen in Figure 3. The key that kept secret has been agreed between the sender and the recipient is used for encryption using the Playfair cipher as described in the Playfair cipher algorithm. Vigenere cipher can still be solved by the method of exhaustive search when the key length is known as the next key is the repetition of the key when the key length is not equal to the length of plaintext. To overcome these drawbacks, the method used to randomize the sequence of next key using key stream generators. The formula used to generate a key using the key stream is

$$Ki = K(i - 1) + K(i - m) \bmod 256 \qquad (1)$$

For example, if the plaintext is known as image with the intensity of 73 78 70 79 82 77and the key used is 73 83 84, then the key used for encryption should be added 3 key elements to a key length equal to the length of the plaintext. The 4th up to 6th key obtained as follows:

k4 = (k3 + k1) mod 256 = (84 + 73) mod 256 = 157

k5 = (k4 + k2) mod 256 = (157 + 83) mod 256 = 240

k6 = (k5 + k3) mod 256 = (240 + 84) mod 256 = 68

While the key used for encryption using vigenere cipher generated from keys along the next n+1 to n keys with key m x n using the key stream generator in equation (1). Image encryption steps as follows:

(i) Select the Playfair key agreed between the sender and the recipient.

(ii) Generating vigenere key with steps:

a. Take the value of playfair key element of the matrix at position (1,1) e.g. is worth 82.

b. Playfair key along 82 elements drawn from Playfair key element of the position (1,1) toposition (5,2). Key value at position 83 to the n-th (n = number of rows * number of columns of the matrix image that will be encrypted) generated by the method of keystream generators in equation (1).

(iii) Insert the image that will be encrypted

(iv) Gray scale images do not need the colour transformation.

(v) Perform encryption using a vigenere key for our image followed by playfair key

Two examples are given in fig 5 and fig 6 which shows the encrypted and decrypted images for different passwords.

Note: If the random key we are entering at encryption and decryption will be are same then we can get back our original image.

Decryption

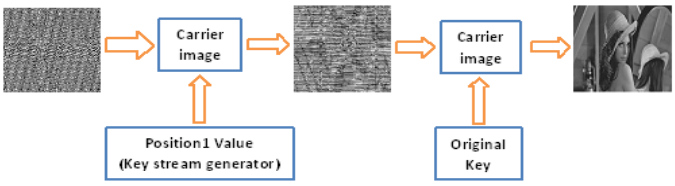


Figure 4 Process of decryption

Decryption algorithm

Decryption process can be seen in Figure 4. Image decryption steps as follows:

(i) Insert the image that will be decrypted

(ii) Select a key that will be used to decrypt the image using the method of Playfair, then generate a key to decrypt the image using the method of vigenere on image in the same way with the encryption process.

(iii) Perform decryption process using Playfair method with similar step in the encryption.

(iv) Now apply vigenere cipher to the result obtained.

(v) If same random key is used while encryption and decryption so our original image can be obtained

4. RESULT IMAGES

ENCRYPTION PASSWORD: **andhrauniverity**


(original image)


(encrypted image)

DECRYPTION PASSWORD: **andhrauniversity**

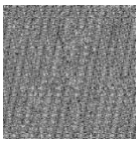

(decrypted image)

ENCRYPTION PASSWORD: **andhrauniverity**


(original image)


(encrypted image)

DECRYPTION PASSWORD: **srkrengcollege**

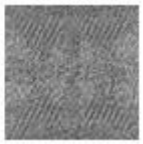


(decrypted image)

Figure 5 Encryption and decryption for 'Lena' image

ENCRYPTION PASSWORD: **srkr@2014**

(original image)



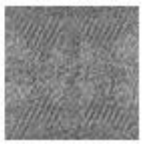
(encrypted image)

DECRYPTION PASSWORD: **srkr@2014**

(decrypted image)

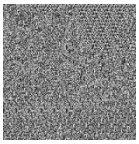
ENCRYPTION PASSWORD: **srkr@2014**

(original image)



(encrypted image)

DECRYPTION PASSWORD: **andhrauniversity**



(decrypted image)

Figure 6 Encryption and decryption for 'Natural Building' image

5. RESEARCH METHOD

This study is generally divided into two phases. The first stage is the design and analysis of the proposed encryption algorithm. Algorithm analysis was performed using Mat lab, Super Encryption is one of the character-based cryptography that combines two ciphers. It aims to gain a stronger cipher so it is not easy to solve, and also to address the use of a single cipher which comparatively weak. In this study, the process of encryption and encryption on both Vigenere ciphers and Playfair cipher were performed with one-time processor each cipher. To determine whether the proposed encryption algorithm is safe enough to be implemented, performed analysis and testing of the encryption algorithm uses several parameters, namely-

Quality of Encryption:

Measurement of the encryption quality is done by comparing the pixel values before and after the encrypted image. The higher rate of change of pixels, then the image encryption is said to be more effective and more secure. The size of the encryption quality is expressed as the deviation between the plain image and cipher image. Encryption quality represents the average number of changes per degree of gray. To measure the quality of the encryption used the formula:

$$EQ=\frac{\sum_{l=0}^{255}|Hl(c)-Hl(p)|}{255}$$

Where:
EQ: quality of encryption
p: plain image, *c*: cipher image, *l* : gray scale
Hl (p): No. of occurrences for each L in a plain image
Hl(c): No. of occurrences for each L in a cipher image

Quality of encryption value for different passwords:

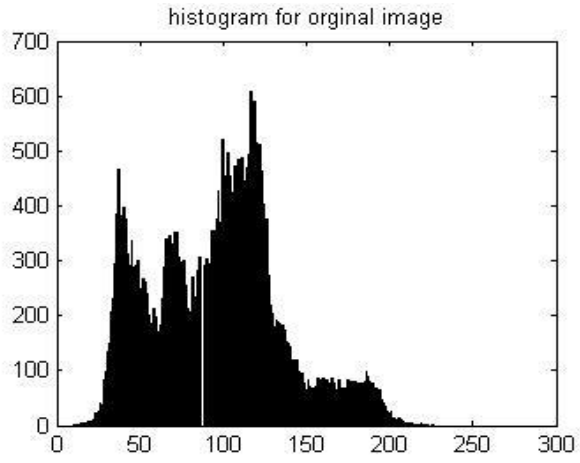
Password: Andhrauniversity
Quality of encryption value-154.47

Password: indiazmycountry
Quality of encryption value-140.83

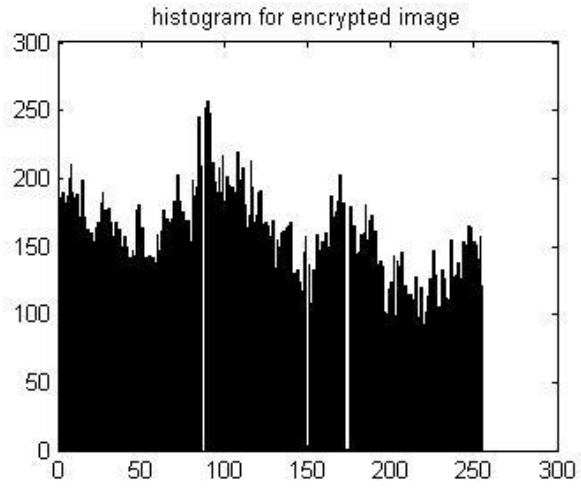
Histogram Analysis

Histograms

Encryption password: srkrece@2014



(a)



(b)

Figure 7 Histogram for (a) Original image (b) Encrypted image

Histogram analysis used to find out image pixel intensities values graphically. Fig 7 shows the histograms for original image and encrypted image, So that we can see how far the intensity values had been rearranged. Colour histogram analysis technique is used to view the suitability of the colour distribution between plain image and cipher image. If the histogram value has a significant distribution of diversity of cipher image and also have significant differences with plain image histogram, it can be said that cipher image does not give any clues to perform statistical attack on the encryption algorithm.

6. CONCLUSION

The test results show that visually the encrypted image is not visible any more due to pixel randomization and intensity changes significantly. From the histogram of plain image and cipher image was seen a significant difference between both of them. The average quality of encryption of indicates that the rate of change of pixels change is high enough so that this system can be said to be effective and safe. This super encryption algorithm can be applied to colour images also. Entropy and Correlation can be performed to assess the quality of Image encryption. It can be implemented to mobile devices also because of fewer complexions.

REFERENCE

1. D. Kahn, The Code breakers: The Story of Secret Writing, New York, Macmillan Publishing Co., 1967.
2. G.Prasanna Lakshmi, Dr. D.A.Chandulal, Dr.KTV Reddy "An improved visual cryptography scheme for secret hiding", International Journal of Computer Science and Information Security, Vol. 9, No. 3, March 2011.
3. K.Sakthidasan and B.V.Santhosh Krishna "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011.
4. Chao Shen Chen and Rong Jian Chen, "Image encryption and decryption using SCAN methodology," Proc. PDCAT, 2006.
5. Xinpeng Zhang, *Member, IEEE*, Guorui Feng, Yanli Ren, and Zhenxing Qian "Scalable Coding of Encrypted Images" IEEE transactions on image processing, vol. 21, no. 6, June 2012.
6. Panduranga H.T, Naveenkumar S.K, "A novel 3-step combinational approach for image encryption", IJCEIT, vol 03, 2009.
7. Sinha, K. Sing., "A technique for image encryption using digital signature"., Optics Communication" , 218, pp.229-234, 2003.
8. Panduranga H.T, Naveenkumar S.K, "A novel image encryption method using 4outof8 code", proc. ommV'09, pp 460-462, 2009.
9. G. Nagaraju, T. V. Hymalakshmi "Image Encryption using Secret-Key images and SCAN Patterns" Int. J. of Advances in Computer, Electrical & Electronics Engg., Vol. 2 , pp. 13-18, Dec. 2012.